REMARKS/ARGUMENTS

In the response to the Office Action mailed December 20, 2005, Applicants propose to amend their application and request reconsideration in view of the proposed Amendment and the following remarks. It is proposed in this Amendment to cancel claims 5 and 6 with the result that claims 4, 7, and 11-20 will remain pending upon entry of this Amendment. It is not proposed to amend any remaining claim.

Claims 5 and 6 were rejected as unsupported by the original disclosure, pursuant to 35 USC 112, first paragraph. According to the Office Action, various elements of claim 5 as previously presented are not disclosed in the patent application as filed. Applicants respectfully disagree and believe that the Examiner intended to state that he did not find verbatim support for amended claim 5 in the specification. It is well understood in U.S. patent application prosecution practice that a claim does not have to have verbatim support in a patent application to meet the requirements of 35 USC 112, paragraph 1. Rather, the subject matter of the claim must be disclosed in the patent application as required by 35 USC 112. The disclosure necessary to support claims 5 and 6 is present in the patent application. Nevertheless, in an attempt to conclude the prosecution of this patent application, claims 5 and 6 are cancelled. It is apparent that the minor error in claim 6 could be cured simply by adding the "of the" before the final word of that claim. However, in view of the dependency of claim 6 from claim 5, and the desire to complete the prosecution of this patent application, claim 6 is also proposed to be cancelled.

In the two fundamental rejections of the claims pending in this patent application, the Office Action makes reference to claims 8-10, claims that were previously cancelled. It is understood that the rejections in the Office Action are correctly stated except for the inadvertent error in referring to cancelled claims 8-10.

There are three pending independent claims in the patent application, as acknowledged in the Office Action, claims 15, 18, and 20. Those three independent claims were all rejected as anticipated both by Batson et al. (U.S. Patent Application 2002/0169874, hereinafter Batson) and by Kawan et al. (Published U.S. Patent Application 2001/0049785, hereinafter Kawan). Both of these rejections are respectfully traversed. While certain dependent claims were rejected as anticipated by Batson and Kawan and claim 17 was rejected as obvious over either of Batson or Kawan in view of a secondary reference, it is apparent that the propriety of all rejections depends upon the assertion that each of the independent claims is anticipated by at least one of Batson and Kawan. Therefore, the following discussion focuses on the rejections of the independent claims as anticipated and demonstrates the error in those rejections. Accordingly, those rejections must be withdrawn and, upon that withdrawal, the remaining rejections cannot be maintained. Accordingly, no discussion of the rejections of the dependent claims is necessary nor provided here.

Each of the three independent claims, as noted, includes four similar, if not identical, limitations. Claim 20, a method claim, provides a useful example of those limitations. Of course, claim 20 includes a further limitation not part of independent claim 18 and claim 15 is directed to a system in which parallel limitations directed to particular "means" are included. The point of the comparison of the limitations of claim 20 to Batson and Kawan is to demonstrate that none the pending claims is described by anything in either of Batson or Kawan.

The limitations of interest from claim 20 are:

> inputting respective accuracy thresholds for each of the authentication devices;
>
> inputting target identification accuracy for the authentication system in identifying a person supplying biometric indicia through the authentication devices;
>
> calculating identification accuracy in identifying a person using biometric indicia input through the respective authentication devices, based on the accuracy thresholds input, for each of the authentication devices, considered individually and for at least one combination of at least two of the authentication devices;
>
> selecting for use in the authentication system only the authentication devices and combinations of authentication devices having calculated identification accuracies meeting the target identification accuracy of the authentication system that has been input;

These limitations were described in prose at page 8 of the previous response. Part of that description is reproduced. The system provides an input means, such as a keyboard, for inputting and storing accuracy thresholds for each of the authentication devices. Specifying the accuracy thresholds causes the error rates of the authentication devices to be established at particular levels as described in connection with Figures 4A and 4B of the patent application. The system also provides for input of a target identification accuracy for the system. This target identification accuracy permits the administrator of this system to establish different levels of security for different degrees of access. Higher security means that the identification accuracy must be higher so that no persons or very few persons are granted access to which they are not entitled. Further, a very important aspect of the invention is that the system calculates, considering the accuracy thresholds for each of the authentication devices, the identification accuracy for the respective authentication devices as well as for combinations of those devices. Then, based upon the calculated identification accuracies of the individual authentication devices and combinations of authentication devices, the system selects for use in a particular application only those individual authentication devices or only the combinations of the individual authentication devices that meet the minimum system target identification accuracy that has been input. An authentication system tailored to a particular need and using the available authentication devices is thus configured.

Applicants acknowledge that Batson and Kawan are in the field of the present invention and may even be directed to solving the same problem that is solved in the invention. However, the descriptions and solutions of Batson and Kawan are different from the claimed invention and cannot, therefore, anticipate the claimed invention. In applying Batson, the Examiner directed attention to paragraphs [0020]-[0025] of Batson as well as to Figure 3 of Batson. Figure 2 of Batson is likewise of significance, particularly in view of the citation of paragraph [0025] of Batson in the Examiner's reply to the previous arguments.

In order to apply any part of Batson to the cited limitations, certain functions in Batson that are not expressly described must be implied. Even making these implications, the limitations of the claims are not met. There is no express description in Batson of determining respective accuracy thresholds for each of the authentication devices of Batson. Batson describes collecting not only biometric information but also much non-biometric information, such as information from a smart card, a user identifier, a password, and other indicia that can be much more easily forged or counterfeited than the biometric data. Of course, according to Figure 3 of Batson, a "security level" is established for input information for various authentication indicia but not for any particular device as in the invention. (The present invention does not contemplate a password, for example, as an authentication device or index but, for the purposes of this argument, it is assumed that the computer system acting on an input password or decrypting some information might be compared to an authentication device. This assumption is made only for the purposes of responding to the rejection and is not a statement that a password checker corresponds to any authentication device according to the invention.) Moreover, there is no indication of any accuracy threshold for any of the authentication tests indicated in Figure 3 of Batson, only a "security level", a term that has no definition in Batson and that has no ordinary meaning nor reference, unlike the accuracy thresholds that are input according to the invention. Thus, it is clear that Batson fails to meet the first of the limitations listed above and cannot anticipate any pending claim.

According to paragraph [0021] of Batson, after a user has been authenticated, the method by which the authentication was achieved is used "in combination with other access characteristics and administrator configured security levels to determine whether to permit access to the requested service." This process of Batson has so little relationship to the second through fourth limitations of the part of claim 20 cited above that comparison of this feature of Batson to the claimed invention is extraordinarily difficult. In Batson, there appears to be a multiple step process of first identifying a person, possibly employing biometric data. In that process, after considering the kind of information employed to identify the person, perhaps involving the accuracy of the identification, although no such statement appears in Batson. That information is used in a way not explained in Batson "to provide access to the requested service based on the security level associated with the requested service and the access characteristics of the session." All that can be gleaned from this description in Batson with respect to the limitations listed above is that, apparently, an administrator establishes security levels, such as shown in Figure 3 of Batson, and uses the security levels, which have an unexplained relationship to the accuracy of the personal authentication, to determine whether to grant access to a requested service.

An important point in attempting to understand the confusing disclosure of Batson is that Batson never describes, as in the invention, inputting target identification accuracy for the authentication system that determines the accuracy of authenticating a particular person seeking access. Rather, in Batson the person is authenticated in some unknown way and then the accuracy of the authentication is questioned, based upon the particular data employed in the authentication. Thus, the second of the cited limitations of the independent claims is not met and it follows that the third limitation, calculating identification accuracy, "based on the accuracy thresholds...for each of the authentication devices, *considered individually and for at least one combination of at least two of the authentication devices*" cannot have any counterpart in Batson.

As made clear in the flowchart of Figure 2 of Batson and described in paragraph [0025] of Batson, it is not the accuracy characteristics of the authentication devices that are employed in Batson in attempting to ensure proper identification of an individual and to determine which individuals may gain access to limited-access locations or information. Rather, as shown in step 202 of that flowchart, security levels, which may somehow relate to accuracy of identification, are not associated with the devices collecting biometric data but are associated with combinations of "access characteristics", another term that is not explained in Batson. In step 204 of Figure 2 of Batson, available services, meaning information with different degrees of access limitations, are then associated with Batson's security levels. At best, parts of Batson are inverted with respect to the claimed invention.

Further, Batson never contemplates using accuracy thresholds of respective authentication devices, taken in combination as well as individually, to determine how accurately a person has been identified and, thereby, to determine which biometric data and associated authentication devices are to be used, individually or in combination, in ensuring that a person is accurately identified for association with a particular access level.

In fact, the final important feature of the limitations cited above, i.e., selecting for use in a particular authentication system only those authentication devices and combinations of authentication devices that can provide a calculated accuracy in personal identification, has no counterpart in Batson, even considering the different vocabularies used in the present patent application and in Batson. Perhaps the most similar passage in Batson appears at the end of paragraph [0021], providing for the introduction of "new security mechanisms". When new security mechanisms, a term likewise not explained by Batson, are introduced, then an administrator can adjust access characteristics, security levels, and services. This unexplained feature of Batson is simply too vague to assert that it describes the calculating and selecting features of the final two claim limitations reproduced above and to assert that these features are described, i.e., anticipated, by Batson. In fact, these two features are so different from what is described in Batson that not even a rejection for obviousness based upon Batson could be proper.

Applicants note the Examiner's reply, referring to Figures 2 and 3 of Batson and its paragraph [0025]. While that paragraph of Batson may state, as quoted by the Examiner, that Table 302 of Figure 3 is only exemplary with regard to "possible access characteristics" and possible combinations that could be used to define access privileges, those statements still do not align with the specific limitations of the pending claims reproduced above, much less disclose those limitations. Applicants agree that Figure 3 of Batson does show combinations of security measures, but not "authentications", that have associated "security levels", or "associated identification accuracy levels", the terms of the claims. The Examiner has interchanged these terms, which clearly have different meanings in the present patent application and its claims and, to the extent identifiable, in Batson.

Applicants agree that the "security levels" of Figure 3 of Batson are somehow employed, in a way that is not explained in Batson, as part of a determination of access privileges. However, there is no congruence of these comments and the limitations of the independent claims identified above. Further, Batson does not include any description of calculating identification accuracy based upon accuracy thresholds for each of authentication *devices*, considered individually, ***and for at least one combination of at*** *least two of the authentication devices*", nor the selection of such devices from which information is obtained in order to meet the target identification accuracy, as in the invention.

Kawan is more remote from the invention than is Batson. In citing Kawan, the Examiner directed attention to paragraphs [0029]-[0033] of Kawan. Kawan relies on biometric data to a greater degree than Batson in attempting to identify, i.e., authenticate, a person. The reliance is not exclusive, however. Kawan recognizes that collecting multiple biometric data, for example several fingerprints, can enhance the accuracy of identification of a person. According to Kawan, this technique provides "greater security". Nevertheless, the relationship of Kawan to the invention is confined to that concept and, of the cited paragraphs, to paragraph [0033] of Kawan. There, storage of "authentication parameters" is described, although the term "authentication parameters" seems not to be defined in Kawan. As best can be understood, the authentication parameters are the previously registered fingerprints and other biometric and non-biometric data to be compared to input information when a person applies for recognition, i.e., authentication.

Perhaps the paragraph in Kawan most pertinent to the invention, as defined by the pending independent claims, appears in paragraph [0049], a paragraph not mentioned in the Office Action. That paragraph refers to threshold levels of matching fingerprints, meaning matching of a stored fingerprint versus a newly input fingerprint, and discusses adjusting the degree of agreement required for identification by a host computer, depending upon the risk of an error in identification.

However, neither the paragraphs of Kawan cited by the Examiner nor paragraph [0049] describes any of the four limitations of each of the independent claims that are reproduced above from claim 20. At best, paragraph [0049] describes inputting and adjusting a target identification accuracy. There is no description of inputting accuracy thresholds for the variety of authentication devices mentioned by Kawan, calculating identification accuracy based on those accuracy thresholds that are input, for each of the authentication devices considered individually and in at least one combination of those authentication devices, nor selecting amongst the authentication devices to configure a system to ensure meeting a target identification accuracy. The relationship of Kawan to the claimed invention is so tenuous that the anticipation rejection is clearly erroneous and cannot properly be maintained.

Applicants do not disagree with the Examiner's reply concerning Kawan and appearing at the third paragraph on page 11 of the Office Action. However, that description of Kawan, while accurate in itself, does not conform to any part of the invention as defined by the pending claims. The reply, in fact, further confirms that Kawan cannot anticipate nor even suggest any claim now pending.

Upon reconsideration, the rejections should be withdrawn as to the remaining claims and those claims should be allowed. While, in this Amendment, claims are cancelled, no remaining claims are amended. Accordingly, if the rejection should be maintained, the Amendment must be entered for purposes of appeal.

Reconsideration and allowance of the remaining claims are earnestly solicited.

Respectfully submitted,

Jeffrey A. Wyand, Reg. No. 29,458
LEYDIG, VOIT & MAYER
700 Thirteenth Street, N.W., Suite 300
Washington, DC 20005-3960
(202) 737-6770 (telephone)
(202) 737-6776 (facsimile)

Date: March 7, 2006
JAW:ves